Internet Society's Symposium on Network and Distributed System Security'98

On the Problem of Trust in Mobile Agent Systems

U. G. Wilhelm

L. Buttyàn & S. Staamann

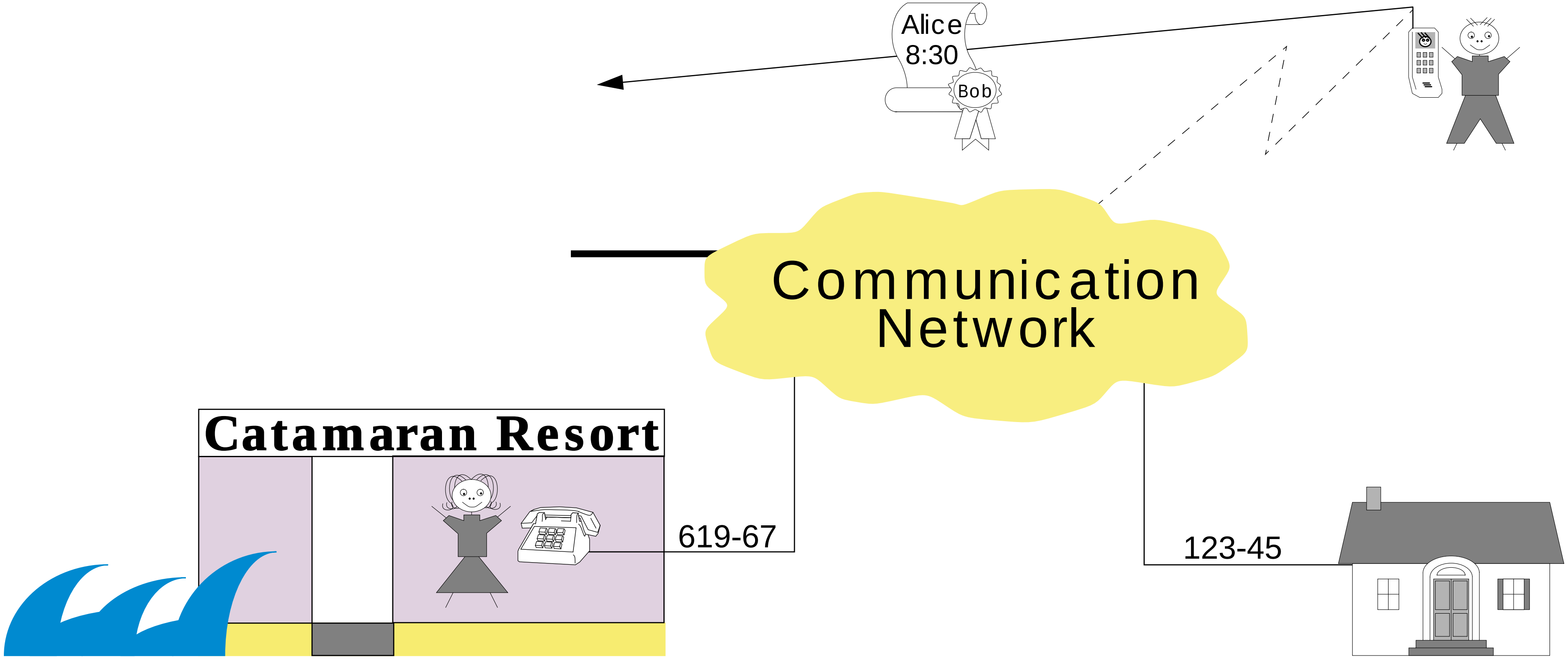
Swiss Federal Institute of Technology, Lausanne (EPFL)

Main Research Interest

protection of personal data & privacy

➪ address the problem from a technical angle.

Example: *call forwarding service*

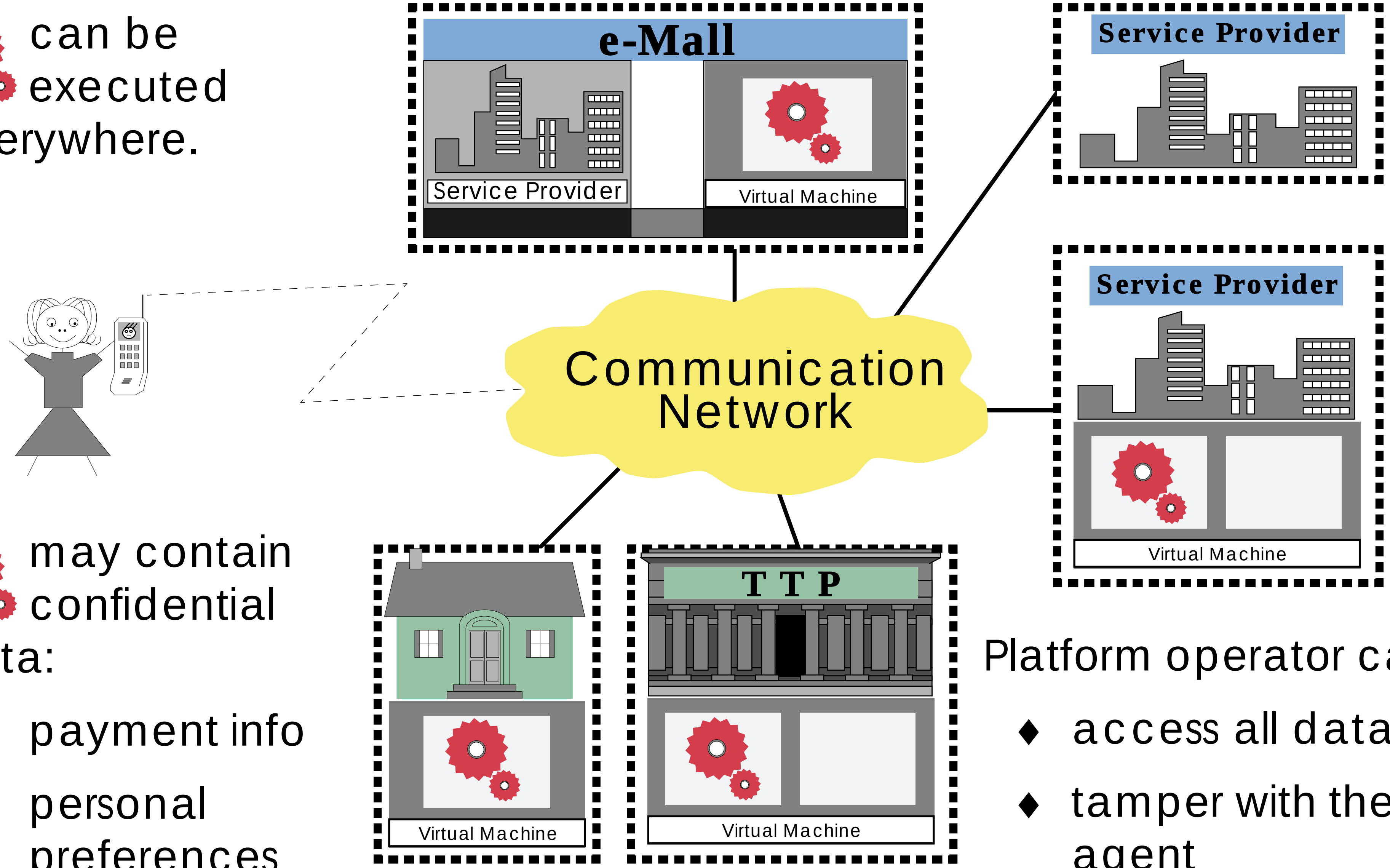


Overview

- ♦ Introduction to the Problem ✓
  - Agents ✓
- ♦ Problem with Agents
- ♦ Definition of Trust
- ♦ The Approach: TPE & CryPO
- ♦ Example
- ♦ Conclusion

The World of Agents

⚙ can be executed everywhere.



⚙ may contain confidential data:

- payment info
- personal preferences

Platform operator can:

- access all data
- tamper with the agent

Trust is a Major Issue

- Secure systems always rely on some form of trust.
- Definition is mostly left to intuition.

Some “well understood” forms of trust:

- trust in one’s own family
- trust in employer

Observations

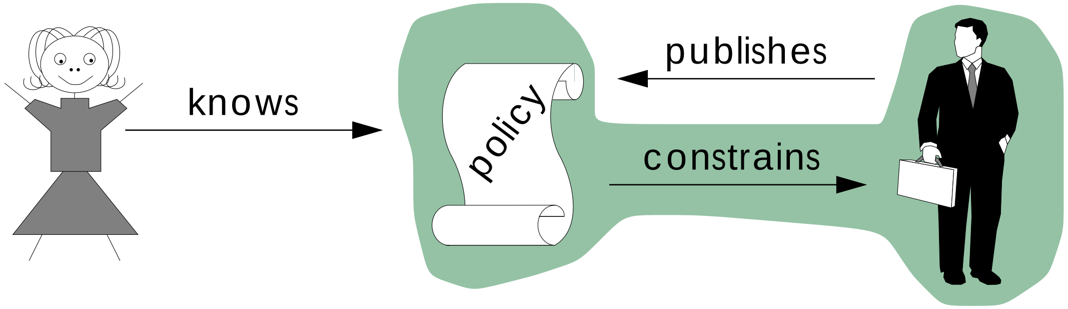
- Trust is rather a social than a technical issue.
- Trust mixes the goals of a principal with its behaviour.
- Goals of a principal are not always clearly stated.

Definition of Trust

- ♦ Goals are made explicit in a policy (set of rules).
- ♦ Policy constrains the behaviour of the principal.
- ♦ Policy is widely known (available to everyone).

Definition:

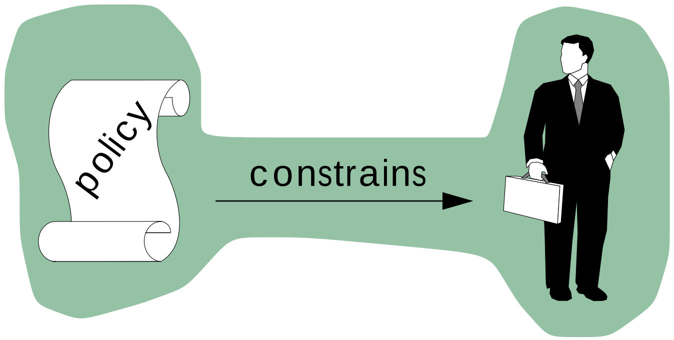
> *Trust in another principal is the belief that it will adhere to its published policy.*



Foundations for Trust

To trust another principal we have to

- verify its published policy
- establish a foundation for the belief that it will adhere to its policy



The belief can be founded on:

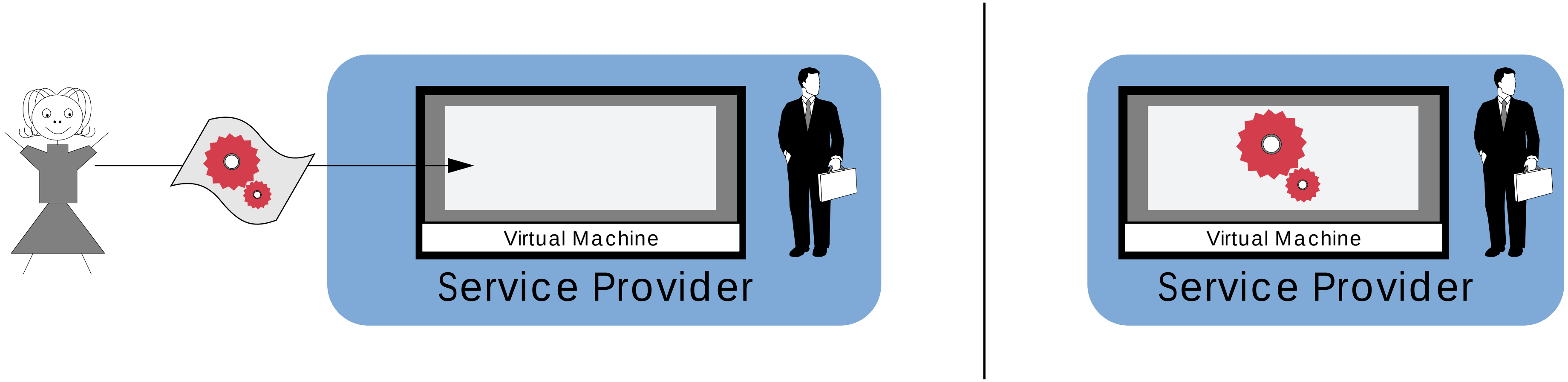
- blind trust
  relies solely on assertion by principal
- good reputation
  principal has a lot to lose if violation is discovered
- control and punishment
  principal is severely punished if violation is discovered
- policy enforcement
  principal *cannot* violate its published policy

What is Policy Enforcement

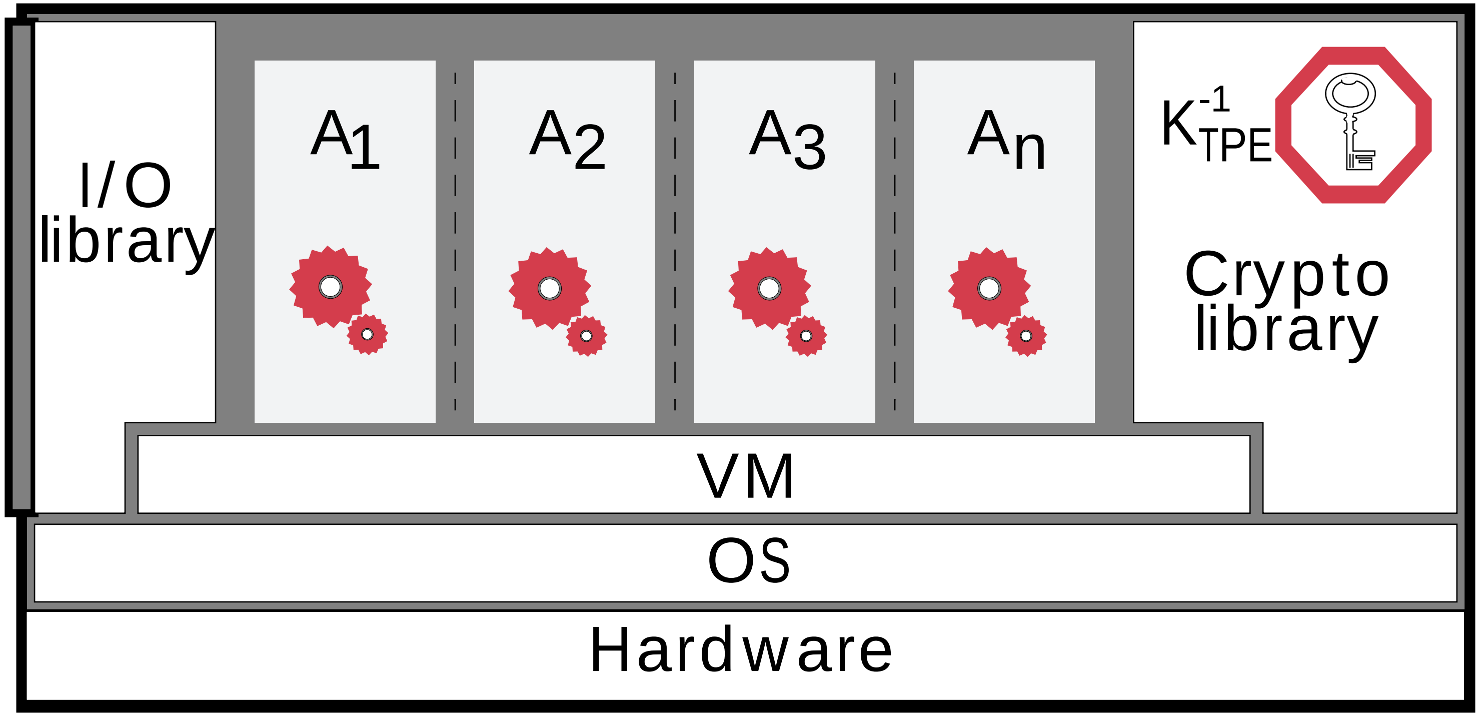
A service provider might have the following rules in his policy:

- ♦ we will not look at your agent’s data (or code) other than what is accessible via its interface
- ♦ we will execute your agent correctly according to its code
- ♦ we will query your agent and encrypt it before sending it off the agent can verify the credentials of the other service provider

➪ this can be enforced with tamper-proof hardware:



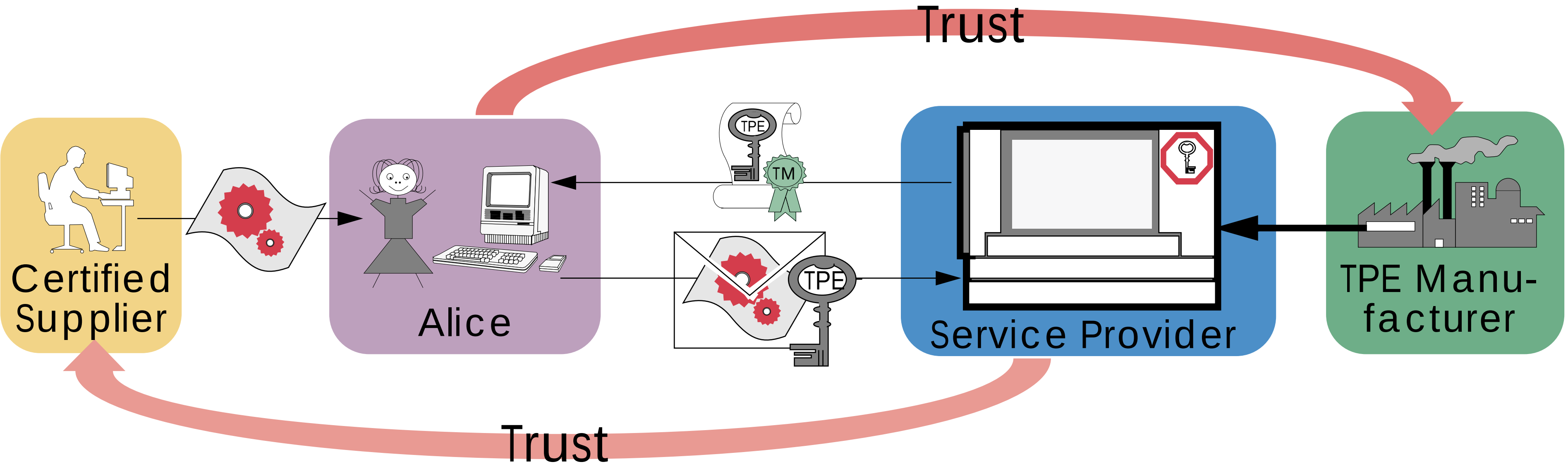
The TPE



- is physically *tamper-proof*
- contains (very) private key
- from trustworthy Manufacturer (certified by institutions)
- provides execution environment for agents (VM)
- well defined interface for interaction with TPE (load/remove of agents)

Transfer of the Agent (CryPO)

- relies on tamper resistance and correctness of the TPE



- Alice obtains an agent (certified supplier)
- Alice configures the agent (e.g., personal data, shared key)
- Alice obtains the certified *public key* of the TPE
- Alice encrypts the agent and sends it to the service provider
- Service provider can not decrypt it — but only load it on the TPE

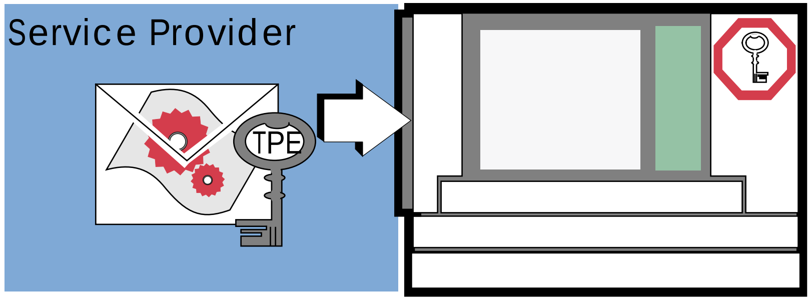
Possible Guarantees

The agent

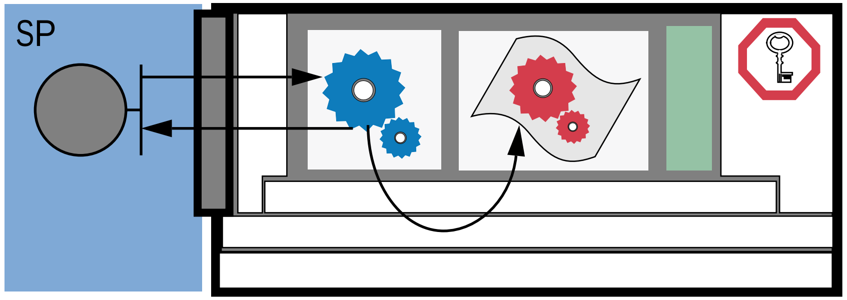
- is protected against tampering and disclosure (code & data)
- can rely on its programmed methods
- can implement at-most-once execution (see paper)
- can follow a defined itinerary (quite complex)
- can implement a limited lifetime (next slide)

Agent Execution (limited lifetime)

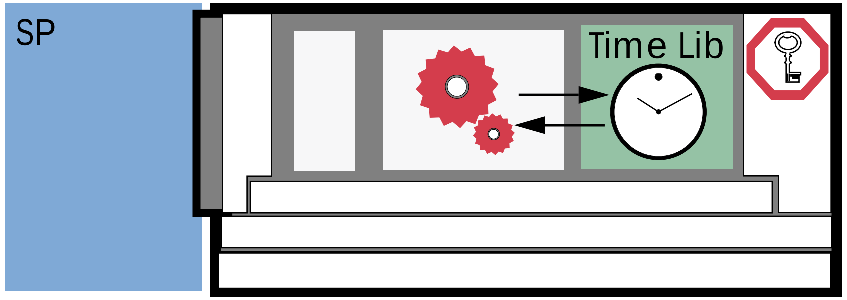
reception of agent



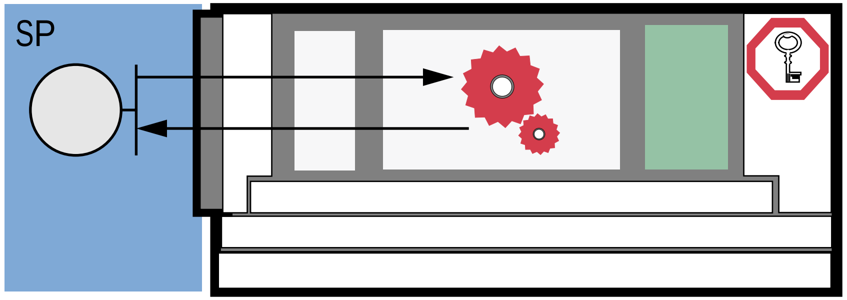
verification of agent



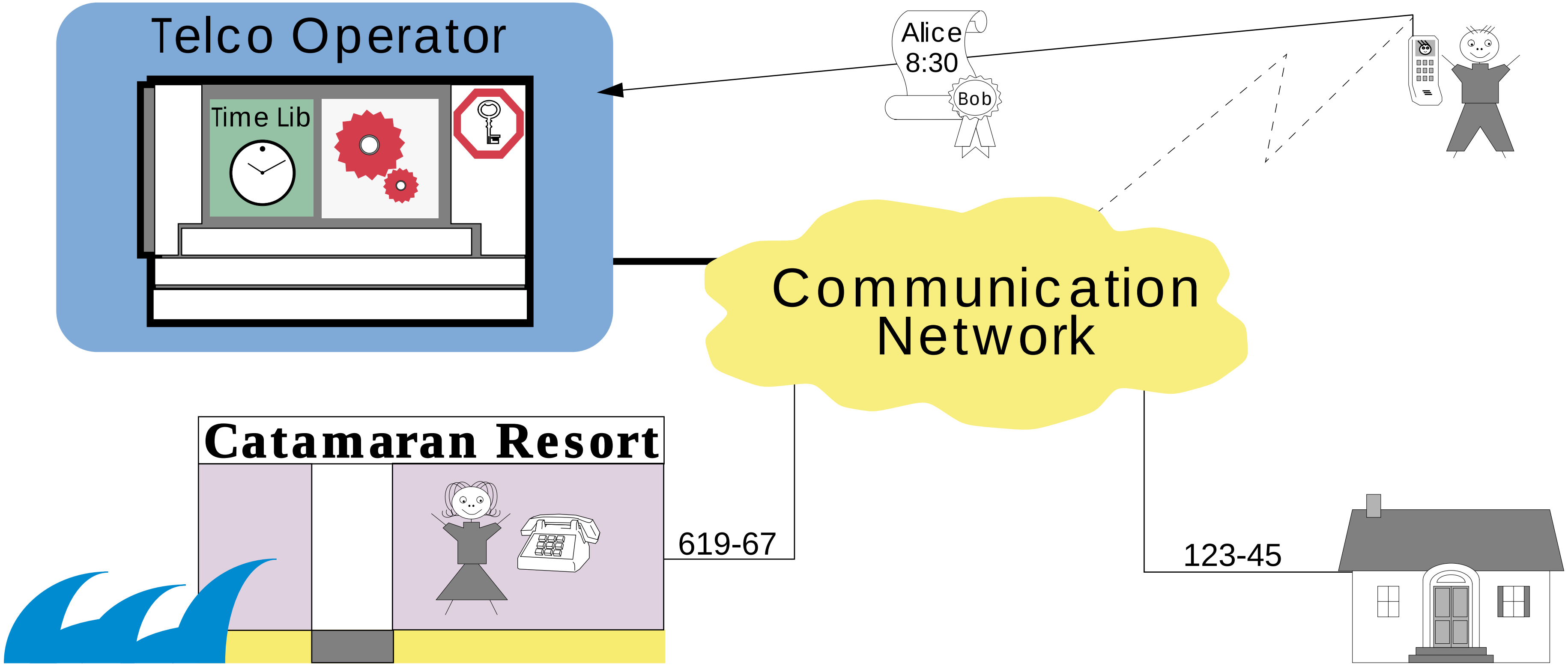
lifetime check by the agent



agent execution



Call Forwarding Service Revisited



- code and data is protected
- Alice sends location updates
- Telco Operator can not access location information

- agent obtains relevant info
  - request & authentication token
  - current time, etc.
- it decides if location is disclosed

Why should we trust the TPE Manufacturer

We cannot enforce correct production at TPE manufacturer

➪ we traded one dependability against another?

Advantages:

- better understanding of security and privacy problems
  specialized service provider
- centralized control
  expert appraisal organizations (small number of TMs)
- resources to build reputation
  TMs are major corporations
- separation of concern
  TM has nothing to gain by misbehaving

The approach favours ***open systems***: small service providers can leverage the trust in reputable TPE manufacturers

➪ clients are more eager to trust.

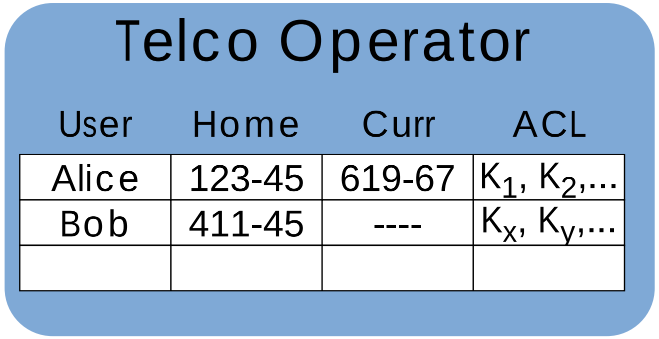
Conclusion

The presented approach

- allows conception of ***open systems***
  trust can be bought
- tries to prevent malicious behaviour rather than correct it
  important for international services
- allows to provide more transparency for users
- is more appropriate to the ideas of the Internet

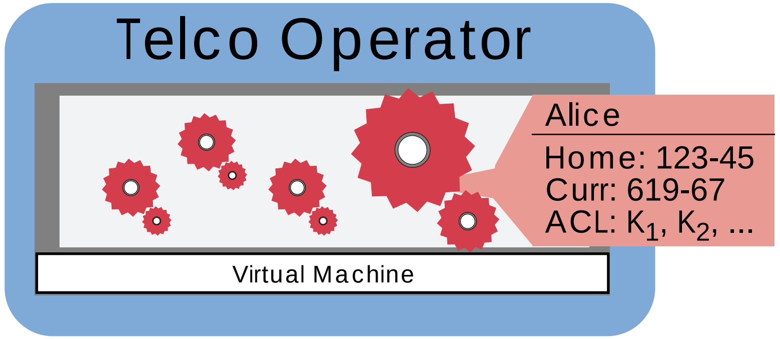
Problems:

- TPE is difficult and expensive to build
  up to now: *vaporware*



Telco Operator

User	Home	Curr	ACL
Alice	123-45	619-67	K_1, K_2,...
Bob	411-45	----	K_x, K_y,...


Telco Operator
Alice
Home: 123-45
Curr: 619-67
ACL: K_1, K_2, ...
Virtual Machine